

MARCELLUS MCRAE, SBN 140308  
mmcrae@gibsondunn.com  
GIBSON, DUNN & CRUTCHER LLP  
333 South Grand Avenue  
Los Angeles, CA 90071-3197  
Telephone: 213.229.7000  
Facsimile: 213.229.7520

ASHLEY E. JOHNSON, admitted *pro hac vice*  
ajohnson@gibsondunn.com  
GIBSON, DUNN & CRUTCHER LLP  
2001 Ross Avenue  
Suite 2100  
Dallas, TX 75201-2911  
Telephone: 214.698.3100  
Facsimile: 214.571.2900

Attorneys for Defendant AT&T MOBILITY, LLC

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
OAKLAND DIVISION

ROBERT ROSS,  
  
Plaintiff,  
  
v.  
  
AT&T MOBILITY, LLC,  
  
Defendant.

CASE NO. 4:19-CV-06669 (JST)

**DEFENDANT AT&T MOBILITY LLC'S  
REPLY IN SUPPORT OF ITS MOTION TO  
DISMISS**

**Hearing:**

Date: February 12, 2020  
Time: 2:00 p.m.  
Place: 1301 Clay Street, 2nd Floor  
Courtroom 6  
Oakland, CA 94612  
Judge: Hon. Jon S. Tigar

## TABLE OF CONTENTS

	<u>Page</u>
I. Introduction.....	1
II. Argument.....	1
A.    Mr. Ross Does Not Adequately Plead Proximate Cause. ....	1
1.    Mr. Ross Failed To Plead Critical Steps in the Supposed Theft of His Funds. ....	1
2.    AT&T Cannot Be Held Liable for the Independent, Intervening Acts of Third Parties. ....	4
B.    Mr. Ross Cannot Defend His Right To Privacy Claim under the California Constitution. ....	5
1.    Mr. Ross’s Complaint Does Not Plead Facts Plausibly Suggesting AT&T Committed an Egregious Breach of Social Norms. ....	6
2.    Mr. Ross Cannot Identify Any Specific Information Disclosed by AT&T. ....	7
C.    The Economic Loss Rule Bars Mr. Ross’s Negligence and Negligent Supervision Claims. ....	9
D.    Mr. Ross Cannot Rest on an Inference of Reliance. ....	11
E.    Mr. Ross’s Alleged Losses Do Not Qualify under the CFAA. ....	12
F.    Mr. Ross’s Allegations Do Not Support Punitive Damages. ....	14
III. Conclusion .....	15

## TABLE OF AUTHORITIES

Page(s)**Cases**

<i>In re Actimmune Mktg. Litig.</i> , 2010 WL 3463491 (N.D. Cal. Sept. 1, 2010) .....	12
<i>Albin v. Trustmark Ins. Co.</i> , 2013 WL 12191722 (C.D. Cal. Nov. 25, 2013) .....	7
<i>Amarillo v. Dobson Cellular</i> , 58 F.3d 635 (5th Cir. 1995) .....	2
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009) .....	6
<i>AtPac, Inc. v. Aptitude Sols., Inc.</i> , 730 F. Supp. 2d 1174 (E.D. Cal. 2010) .....	13
<i>Bank of Am. Corp. v. City of Miami, Fla.</i> , 137 S. Ct. 1296 (2017) .....	2
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007) .....	1
<i>Blankenhorn v. City of Orange</i> , 485 F.3d 463 (9th Cir. 2007) .....	6
<i>Body Jewelz, Inc. v. Valley Forge Ins. Co.</i> , 241 F. Supp. 3d 1084 (C.D. Cal. 2017) .....	9
<i>California v. Sup. Ct.</i> , 150 Cal. App. 3d 848 (1984) .....	4
<i>Chevron Corp. v. Donziger</i> , 2013 WL 4536808 (N.D. Cal. Aug. 22, 2013) .....	8
<i>Clayton v. Landsing Pac. Fund, Inc.</i> , 2002 WL 1058247 (N.D. Cal. May 9, 2002) .....	12
<i>Coll. Hosp. Inc. v. Sup. Ct.</i> , 8 Cal. 4th 704 (1994) .....	14
<i>Corona v. Sony Pictures Entm't, Inc.</i> , 2015 WL 3916744 (C.D. Cal. June 15, 2015) .....	10
<i>Cruz v. HomeBase</i> , 83 Cal. App. 4th 160 (2000) .....	14
<i>Daugherty v. Am. Honda Motor Co., Inc.</i> , 144 Cal. App. 4th 824 (2006) .....	12
<i>DocMagic, Inc. v. Ellie Mae, Inc.</i> , 745 F. Supp. 2d 1119 (N.D. Cal. 2010) .....	12

## TABLE OF AUTHORITIES

(continued)

	<u>Page(s)</u>
<i>Fieldstone Co. v. Briggs Plumbing Prods., Inc.</i> , 54 Cal. App. 4th 357 (1997) .....	10
<i>Figy v. Amy's Kitchen, Inc.</i> 2013 WL 6169503 (N.D. Cal. Nov. 25, 2013).....	11, 12
<i>In re Google Location History Litig.</i> , 2019 WL 6911951 (N.D. Cal. Dec. 19, 2019) .....	8
<i>Hill v. Nat'l Collegiate Athletic Ass'n</i> , 7 Cal. 4th 1 (1994) .....	6
<i>Imber-Gluck v. Google, Inc.</i> , 2014 WL 3600506 (N.D. Cal. July 21, 2014).....	11
<i>In re iPhone Application Litig.</i> , 844 F. Supp. 2d 1040 (N.D. Cal. 2012) .....	8
<i>Kalitta Air, L.L.C. v. Cent. Tex. Airborne Sys., Inc.</i> , 2004 WL 7339814 (N.D. Cal. Aug. 19, 2004).....	9
<i>Low v. LinkedIn Corp.</i> , 900 F. Supp. 2d 1010 (N.D. Cal. 2012) .....	7
<i>Mega RV Corp. v. HWH Corp.</i> , 225 Cal. App. 4th 1318 (2014) .....	11
<i>Modisette v. Apple, Inc.</i> , 30 Cal. App. 5th 136, 155 (2018) .....	4
<i>N. Am. Chem. Co. v. Sup. Ct.</i> , 59 Cal. App. 4th 764 (1997) .....	9
<i>In re Nexus 6P Prod. Liab. Litig.</i> , 293 F. Supp. 3d 888 (N.D. Cal. 2018) .....	4
<i>NovelPoster v. Javitch Canfield Group</i> , 140 F. Supp. 3d 954 (N.D. Cal. 2014) .....	13
<i>Opperman v. Path, Inc.</i> , 87 F. Supp. 3d 1018 (N.D. Cal. 2014) .....	10, 11
<i>Oracle USA, Inc. v. XL Glob. Servs., Inc.</i> , 2009 WL 2084154 (N.D. Cal. July 13, 2009).....	9
<i>Ott v. Alfa-Laval Agri., Inc.</i> , 31 Cal. App. 4th 1439 (1995) .....	10
<i>Perez v. Auto Tech. Co.</i> , 2014 WL 12588644 (C.D. Cal. July 14, 2014) .....	15

## TABLE OF AUTHORITIES

(continued)

	<u>Page(s)</u>
<i>Razuki v. Caliber Home Loans, Inc.</i> 2018 WL 2761818 (S.D. Cal. June 8, 2018).....	9
<i>Rojas-Lozano v. Google, Inc.</i> 159 F. Supp. 3d 1101 (N.D. Cal. 2016) .....	11
<i>Ruiz v. Gap Inc.</i> , 540 F. Supp. 2d 1121 (N.D. Cal. 2008) .....	6
<i>Schneider v. Cal. Dep’t of Corr.</i> , 151 F.3d 1194 (9th Cir. 1998).....	6, 11
<i>Simplicity Int’l v. Genlabs Corp.</i> , 2010 WL 11515296 (C.D. Cal. Apr. 21, 2010) .....	14
<i>SKF USA, Inc. v. Bjerkness</i> 636 F. Supp. 2d 696 (N.D. Ill. 2009) .....	13
<i>In re Sony Gaming Networks &amp; Customer Data Sec. Breach Litig.</i> , 996 F. Supp. 2d 942 (S.D. Cal. 2014) .....	10, 11
<i>Sunbelt Rentals, Inc. v. Victor</i> , 43 F. Supp. 3d 1026 (N.D. Cal. 2014) .....	7, 8
<i>Taamneh v. Twitter, Inc.</i> , 343 F. Supp. 3d 904 (N.D. Cal. 2018) .....	4
<i>Terpin v. AT&amp;T Mobility, LLC</i> , 399 F. Supp. 3d 1035 (C.D. Cal. 2019) .....	3, 4, 5
<i>Toole v. Richardson–Merrell Inc.</i> , 251 Cal. App. 2d 689 (1967).....	14
<i>Tyan, Inc. v. Garcia</i> , 2017 WL 1658811 (C.D. Cal. May 2, 2017) .....	13
<i>United States v. Forrester</i> , 512 F.3d 500 (9th Cir. 2008).....	8
<i>In re Yahoo! Inc. Customer Data Sec. Breach Litig.</i> , 313 F. Supp. 3d 1113 (N.D. Cal. 2018) .....	15
<i>Zamora v. Shell Oil Co.</i> , 55 Cal. App. 4th 204 (1997) .....	9
<i>Zbitnoff v. Nationstar Mortg., LLC</i> , 2014 WL 1101161 (N.D. Cal. Mar. 18, 2014).....	7

## I. Introduction

In his Opposition to AT&T Mobility LLC’s motion to dismiss, Plaintiff Robert Ross relies on conclusory allegations in his Complaint as a substitute for pleading the actual *facts* required to state a plausible claim for relief. For instance, in response to AT&T’s argument that Mr. Ross has not pled proximate cause, he points to the generic allegations in the Complaint regarding SIM swaps and urges this Court to accept those allegations in lieu of allegations about what supposedly happened in this case. But to state a claim for relief, Mr. Ross must plausibly allege that a SIM swap caused his alleged harm, not simply allege that SIM swaps are *capable* of leading to a theft. Because Mr. Ross pleads virtually no facts to support his conclusory assertion that criminal hackers’ “control” of his phone number led to his alleged harm, his Complaint should be dismissed in its entirety.

Mr. Ross also fails to remedy the flaws in several of his specific claims. Instead, at every turn, he asks this Court to accept “labels and conclusions” in place of plausible factual allegations. *See Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). That approach is simply inadequate.

In short, Mr. Ross’s Opposition overreaches in his attempt to blame AT&T for conduct that it did not control and harm that should be assigned to the intentional misconduct of third-party hackers. Mr. Ross’s Complaint should be dismissed in its entirety.

## II. Argument

### A. Mr. Ross Does Not Adequately Plead Proximate Cause.

#### 1. Mr. Ross Failed To Plead Critical Steps in the Supposed Theft of His Funds.

Because the Complaint fails to explain any steps hackers took to turn control over Mr. Ross’s phone number into the withdrawal of millions of dollars from his bank and/or digital account, it does not plausibly allege proximate cause. It is not sufficient, as Mr. Ross urges, to simply assert that hackers “used th[eir] control” over Mr. Ross’s phone number “to access and take control of these accounts of Mr. Ross and control the entire USD amounts he held in both accounts,” Compl. ¶¶ 37–38—much less to assert as a general matter that control over a phone number “can” be used to access and control online accounts, *id.* ¶ 24. Mr. Ross must plead the facts necessary to make it plausible that the SIM swap he alleges in fact led to the purported theft, including such facts as how hackers identified where his money was stored, what security guarded those accounts (including what information other

1 than control of a phone number was needed to access an account), what information the hackers  
 2 necessarily already had before performing the SIM swap, and what role that information played in  
 3 obtaining access to Mr. Ross's accounts. Nothing in Mr. Ross's Opposition addresses this fundamental  
 4 problem. Accordingly, Mr. Ross's claims for damages must be dismissed.<sup>1</sup>

5 As an initial matter, Mr. Ross contends that AT&T "ignores" allegations that "detail[] how a  
 6 SIM swap is much more than a mere transfer of a phone number." Opp. at 2–3. But the Complaint  
 7 alleges that SIM swapping is "a relatively simple scheme, wherein third parties take control of a  
 8 victim's mobile phone number." Compl. ¶ 20. Mr. Ross's conclusory assertion that a SIM swap  
 9 transfers "password reset capabilities" does not undermine this definition. Opp. at 3. Instead, as Mr.  
 10 Ross alleges, transfer of control over a phone number can permit hackers in some circumstances, if  
 11 they possess the right other information, to reset a password for certain websites. See Compl. ¶ 24.  
 12 But the SIM swap does not, by itself, hand to the hacker access to a bank or cryptocurrency account.  
 13 Instead, a SIM swap provides hackers with a tool that itself is neither necessary nor sufficient to steal  
 14 funds. To link the SIM swap to a theft of funds therefore requires allegation that plausibly explain how  
 15 control over a phone number was turned into theft of particular funds. Mr. Ross has not done this.

16 Importantly, Mr. Ross pleads *no facts* making it plausible to conclude that the \$1,000,000 of  
 17 currency he alleges he possessed in his Gemini account and his Coinbase account was obtained because  
 18 of the alleged SIM swap. Instead, he pleads only his conclusion: that third-party hackers obtained the  
 19 \$1,000,000 "[b]y utilizing their control over Mr. Ross' mobile phone number." Compl. ¶ 38. None of  
 20 Mr. Ross's general allegations about the mechanics of two-factor authentication describe how those  
 21 specific funds were actually taken.

22 Mr. Ross's Opposition, like his Complaint, replaces allegations about his particular claim with  
 23 \_\_\_\_\_

24 <sup>1</sup> Mr. Ross incorrectly asserts that proximate cause is not required for federal statutory claims. Opp.  
 25 at 5 n.2. The Supreme Court routinely finds the opposite. *Bank of Am. Corp. v. City of Miami, Fla.*,  
 26 137 S. Ct. 1296, 1305 (2017) ("It is a well established principle of [the common] law that in all cases  
 27 of loss, we are to attribute it to the proximate cause, and not to any remote cause. . . . We assume  
 28 Congress is familiar with the common-law rule and does not mean to displace it *sub silentio* in federal  
 causes of action.") (citations and quotation marks omitted); *Amarillo v. Dobson Cellular*, 58 F.3d 635  
 (5th Cir. 1995) (affirming judgment where jury was instructed on proximate cause under FCA).  
 Moreover, contrary to Mr. Ross's assertion, AT&T certainly does "dispute" Mr. Ross's allegation that  
 AT&T "violated the [FCA] and . . . is liable to Mr. Ross for damages available under the Act." Opp.  
 at 5 n.2. AT&T simply focuses at the *pleading stage* on the lack of proximate cause.

1 generalities about SIM swaps. Mr. Ross accuses AT&T of “feign[ing] ignorance” of the capabilities  
 2 of SIM swaps and implies that AT&T is arguing that it did not know that SIM swaps present a risk to  
 3 customers. *Id.* at 4. But this is not AT&T’s argument. AT&T has never denied that, under the right  
 4 circumstances, a SIM swap *can* play a role in a theft, or allow an enterprising thief to intercept  
 5 messages. But pleading that SIM swaps can play a role in fraudulent schemes is not a claim for relief.  
 6 To state a claim, Mr. Ross must allege facts plausibly suggesting that a SIM swap *did* proximately  
 7 cause the theft here. On that case-specific point, Mr. Ross simply has nothing.<sup>2</sup>

8 Mr. Ross’ Complaint thus leaves open many questions, requiring the Court and AT&T to guess  
 9 at the answers. Accepting the truth of the Complaint’s factual allegations, hackers obtained control  
 10 over Mr. Ross’s phone number. Eventually, they obtained his funds. But what happened before and  
 11 in between those two events? How did hackers know Mr. Ross had funds in Coinbase, Gemini, and  
 12 Binance accounts? How did they know which cell phone was linked to those accounts (or that any cell  
 13 phone was)? Did they know Mr. Ross’s account number, username, email address, or password? Did  
 14 he have any security question that hackers had to answer? Did he save his password online where it  
 15 could be hacked? What was the role of Authy, a two-factor authentication app, which Mr. Ross alleges  
 16 was used by hackers “to gain access to his cryptocurrency accounts”? *Opp.* at 5. Most importantly,  
 17 did any of his accounts even use a SMS-based two-factor authentication? Notably, all of this  
 18 information is in Mr. Ross’s possession.

19 Federal pleading standards require a plaintiff to do more than ask the court to speculate about  
 20 whether the plaintiff has a claim for relief. Bizarrely, Mr. Ross cites *Terpin v. AT&T Mobility, LLC*,  
 21 399 F. Supp. 3d 1035 (C.D. Cal. 2019), because it did not accept AT&T’s argument that the  
 22 independent, intervening acts of third parties necessarily broke the chain of causation. But Mr. Ross  
 23 \_\_\_\_\_

24 <sup>2</sup> Mr. Ross inexplicably accuses AT&T—twice—of “egregiously misquot[ing] the Complaint” by  
 25 quoting the precise language in paragraph 77 of the Complaint. *Opp.* at 4–5 (citing *Mot.* at 5). The  
 26 quoted language from the FTC states that “[t]he security of two-factor authentication schemes that use  
 27 phones as one of the factors relies on the assumption that someone who steals your password has not  
 28 also stolen your phone number.” *Compl.* ¶ 77. In other words, two-factor authentication is secure *so long as* the same person does not have both factors—i.e., the person “who steals your password has not also stolen your phone number.” *Id.* Given that the language AT&T quoted is the precise language in the block quote in paragraph 77 of the Complaint, it is unsurprising that Mr. Ross does not identify what portion of the direct quote was a “misquote” (or why).



leaves out the key fact that the *Terpin* court *dismissed all damages claims for failure to plead proximate cause*—and it did so in reliance on precisely the arguments and authority AT&T raises here. 399 F. Supp. 3d at 1044 (dismissing Mr. Terpin’s damages claims because “the Court is left to speculate how having access to Mr. Terpin’s phone number resulted in the theft of cryptocurrency”). Mr. Ross does not even *mention*, much less confront, the court’s holding on this point.<sup>3</sup>

Mr. Ross does not cite, and cannot distinguish, directly on point California case law on cited by AT&T in its Motion, which holds that proximate cause does not exist where the “causal link” between alleged negligence and damages is “tenuous at best” because of “several procedural steps” between the negligence and the harm. *California v. Sup. Ct.*, 150 Cal. App. 3d 848, 852–53 (1984); *Modisette v. Apple, Inc.*, 30 Cal. App. 5th 136, 155 (2018) (dismissing complaint because “the gap between Apple’s design of the iPhone and the [plaintiffs’] injuries is too great for the tort system to hold Apple responsible”). This authority confirms the irrelevance of Mr. Ross’s observation that proximate cause is “[g]enerally” a “question of fact for the jury.” Opp. at 3. Where, as here, the complaint fails to plead a plausible chain of causation, dismissal is proper. *See, e.g., Taamneh v. Twitter, Inc.*, 343 F. Supp. 3d 904, 914 (N.D. Cal. 2018) (dismissing a claim because the plaintiff did not plausibly plead proximate cause); *In re Nexus 6P Prod. Liab. Litig.*, 293 F. Supp. 3d 888, 958 (N.D. Cal. 2018) (same); Mot. at 6–7 (citing cases).

## 2. AT&T Cannot Be Held Liable for the Independent, Intervening Acts of Third Parties.

California case law regarding the extent of tort liability for criminal acts is extensive and fact-dependent. *Compare* Mot. at 8–9, *with* Opp. at 5–8.<sup>4</sup> But Mr. Ross has not stated a claim under any standard accepted by California cases.

As set forth above, Mr. Ross has not pled what any hacker did here at a level of specificity that even permits *consideration* of whether that act was foreseeable. The fundamental disconnect is that

<sup>3</sup> In *Terpin*, the plaintiff has filed an amended complaint, the sufficiency of which is currently before the Court on a motion to dismiss.

<sup>4</sup> Mr. Ross errs in dismissing as dicta this Court’s holding in *O’Keefe v. Inca Floats, Inc.*, 1997 WL 703784, at \*4 (N.D. Cal. Oct. 31, 1997), that “independent illegal acts of third parties are deemed unforeseeable and therefore, the sole proximate cause of the injury which excludes negligence of another as a cause of injury.” *See* Opp. at 6 n.3.

the essential question is not whether a SIM swap is foreseeable or could foreseeably lead to certain kinds of harm; it is whether Mr. Ross has plausibly alleged that it was foreseeable to AT&T that this particular SIM swap would occur *and* cause him the particular harm he allegedly suffered. Because the Court does not have before it the chain of events that led from the alleged SIM swap to the alleged theft, it has no means by which to examine whether that chain of events was foreseeable. Mr. Ross’s assertion that “foreseeable intervening events do not absolve a defendant of tort liability,” Opp. at 5, is therefore unhelpful to him. Because the “intervening events” are not pled, there are no facts plausibly suggesting that those events are foreseeable—any fact question, like foreseeability, must be adequately pled before it can possibly go to the jury.<sup>5</sup>

Although Mr. Ross relies on the Central District of California’s decision in *Terpin*, it is not on point. In *Terpin*, the plaintiff alleged that he informed defendant that he was “the victim of a SIM swap” in 2017, which put the defendant on notice that his account was vulnerable months before the damages claimed in the suit were allegedly suffered. 399 F. Supp. 3d at 1044. Based on that previous report, the court concluded that “AT&T was put on actual notice that Mr. Terpin’s account was at risk.” *Id.* Nothing of the sort is pled here.

**B. Mr. Ross Cannot Defend His Right To Privacy Claim under the California Constitution.**

AT&T argued that Mr. Ross’s invasion of privacy claim failed for two reasons. First, he did not allege an egregious breach of social norms because he alleged, at most, that AT&T was negligent. Mot. at 9–10. Second, Mr. Ross did not specify what information AT&T allegedly disclosed, preventing the Court from determining whether he had a reasonable expectation of privacy. Mot. at 10–11. Mr. Ross fails to rebut either argument.

---

<sup>5</sup> For similar reasons, Mr. Ross is incorrect that AT&T “ignores the significance of the word ‘independent.’” Opp. at 6 n.3. “Independent” merely requires that the act be sufficiently disconnected to break the chain of causation, which Mr. Ross’s own definition ties back to whether the intervening criminal acts were “foreseeable.” *Id.* Since Mr. Ross fails to plead what those acts *are*, he has certainly not pled they were foreseeable.

1           **1. Mr. Ross’s Complaint Does Not Plead Facts Plausibly Suggesting AT&T**  
 2           **Committed an Egregious Breach of Social Norms.**

3           As noted in AT&T’s motion, Mr. Ross’s theory in his Complaint is one of negligence. Mot. at  
 4 10. And in his Opposition, Mr. Ross appears to concede that claims of negligence are categorically  
 5 outside the scope of the constitutional right of privacy. Opp. at 9. Having therefore acknowledged that  
 6 the allegations in his Complaint do not state a claim, Mr. Ross now asserts that AT&T employees<sup>6</sup>  
 7 violated company policy by performing a SIM swap, and that “[t]his was not mere negligence . . . it  
 8 was intentional.” *Id.* This is not the Complaint’s theory, and Mr. Ross cannot remedy his failure to  
 9 plead an invasion of the constitutional right of privacy by simply asserting intentional misconduct in  
 10 his Opposition. *See Schneider v. Cal. Dep’t of Corr.*, 151 F.3d 1194, 1197 (9th Cir. 1998) (“[A] court  
 11 may not look beyond the complaint to a plaintiff’s moving papers, such as a memorandum in opposition  
 12 to a defendant’s motion to dismiss.”).

13           Mr. Ross also cannot transform his negligence-based factual allegations into an allegation of  
 14 intentional misconduct simply by labeling them “intentional.” That is precisely the type of “conclusory  
 15 allegation” that is insufficient to state a claim. *Ashcroft v. Iqbal*, 556 U.S. 662, 686 (2009). Mr. Ross’s  
 16 factual allegations are based exclusively on the theory that AT&T did not implement sufficient security  
 17 protocols and did not adequately train its employees—these are negligence claims, not claims of  
 18 intentional wrongdoing. Compl. ¶¶ 46–70, 95–100; *see also Blankenhorn v. City of Orange*, 485 F.3d  
 19 463, 484–85 (9th Cir. 2007) (failure to train an employee “can only be classified as mere negligence”).

20           Moreover, the standard under the constitutional right of privacy is not whether some  
 21 information was intentionally disclosed, but whether the alleged disclosure is an “egregious breach of  
 22 the social norms underlying the privacy right.” *Hill v. Nat’l Collegiate Athletic Ass’n*, 7 Cal. 4th 1, 37  
 23 (1994). While negligent conduct cannot satisfy this standard, simply alleging that a disclosure was  
 24 “intentional” is also not what the law requires. Where information actually disclosed permits merely  
 25 an “increased risk” of harm, that is not an “egregious breach.” *Ruiz v. Gap Inc.*, 540 F. Supp. 2d 1121  
 26 (N.D. Cal. 2008).

27 \_\_\_\_\_  
 28 <sup>6</sup> The individual allegedly performing the SIM swap was not in fact an AT&T employee, but was  
 affiliated with an AT&T vendor.

Here, even if Mr. Ross’s conclusory allegation of intentional conduct were enough to assume AT&T intentionally accessed his account, the extent of that “intent” would be that an AT&T employee (or, more accurately, an individual affiliated with an AT&T vendor) intentionally accessed limited information that Mr. Ross had provided to AT&T. As explained above and alleged in the Complaint, a SIM swap transfers control over a phone number, not information or all contents of a phone, so the Complaint does not plausibly allege that anyone disclosed any information to hackers, intentionally or otherwise. And the Complaint is devoid of any facts or logic to suggest that anyone at AT&T could have intentionally disclosed information they did not have, such as “passports,” “social security numbers, driver’s licenses, birth certificates, and financial information.” Opp. at 10. Accordingly, Mr. Ross has not pled any plausible basis to conclude AT&T violated his constitutional right of privacy.

## **2. Mr. Ross Cannot Identify Any Specific Information Disclosed by AT&T.**

Mr. Ross’s invasion of privacy claim also fails for another independent reason. As noted in AT&T’s initial brief, California courts require invasion-of-privacy plaintiffs to specifically allege what information a defendant disclosed. Mot. at 10–11. Without the required specificity, a court cannot determine whether a plaintiff has a reasonable expectation of privacy in the disclosed information. *See Sunbelt Rentals, Inc. v. Victor*, 43 F. Supp. 3d 1026, 1035 (N.D. Cal. 2014).

Mr. Ross first alleges that AT&T disclosed his Customer Proprietary Network Information (“CPNI”), which he defines as “information about the configuration, type, and use of his AT&T services, his personal information, his SIM card details, and his billing information.” Compl. ¶ 53; Opp. at 9. But none of this information can meet the “high bar” for sustaining an invasion of privacy claim. *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012).

As an initial matter, it is unclear what the term “personal information” encompasses, much less “SIM card details” or “the configuration, type, and use of his AT&T services.” Compl. ¶ 53. Unsurprisingly, the courts do not allow such vague terms to serve as the basis for a violation of the constitutional right of privacy. *See* Mot. at 11; *Zbitnoff v. Nationstar Mortg., LLC*, 2014 WL 1101161, at \*4 (N.D. Cal. Mar. 18, 2014) (private information); *Albin v. Trustmark Ins. Co.*, 2013 WL 12191722, at \*10 (C.D. Cal. Nov. 25, 2013) (financial information). And given that private and financial information has repeatedly been rejected as a basis for a constitutional violation, Mr. Ross’s vaguer

categories must surely fail as well. Indeed, AT&T is aware of no authority suggesting that “SIM card details” or “the configuration, type, and use of . . . AT&T services” is protected by the constitutional right of privacy—and Mr. Ross cites none.

Courts have rejected privacy claims in the cases most analogous to Mr. Ross’s allegations. In *Sunbelt Rentals*, the court held that the plaintiff did not provide enough specificity to sustain his invasion of privacy claim when he alleged that the defendant accessed his “iPhone” and his “private electronic data and electronic communications.” 43 F. Supp. 3d at 1035. Mr. Ross’s category of “SIM card details” is even less specific. And in the context of Fourth Amendment search and seizure—a lower standard than the California constitutional right of privacy<sup>7</sup>—the Ninth Circuit has held that email and Internet users have “no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit,” just like “telephone users have no expectation of privacy in the numbers they dial.” *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008). Email, Internet, and phone users only have a reasonable expectation of privacy in the “underlying contents of communication.” *Id.* Mr. Ross does not allege that hackers obtained access to the contents of communications he sent.

Mr. Ross similarly does not have a reasonable expectation of privacy in his “use of AT&T services,” which reveal nothing about the content of his communications. *In re Google Location History Litig.*, 2019 WL 6911951, at \*10 (N.D. Cal. Dec. 19, 2019) (dismissing as non-specific a claim based on Google’s constant tracking of user’s location and use of its services); *Chevron Corp. v. Donziger*, 2013 WL 4536808, at \*10 (N.D. Cal. Aug. 22, 2013) (“[T]he Court must conclude that the Doe movants have no privacy interest in the subscriber information, IP addresses, and IP logs associated with their email accounts.”); *cf. In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (holding that the disclosure to third parties of unique device identifier number, personal data, and geolocation information did not constitute an egregious breach of privacy).

Mr. Ross also argues that hackers accessed “his and his family’s highly sensitive data, including

---

<sup>7</sup> The California constitution sets “a higher threshold” for showing an expectation of privacy “than for a federal claim under the Fourth Amendment.” *Chevron Corp. v. Donziger*, 2013 WL 4536808, at \*10 (N.D. Cal. Aug. 22, 2013)

color copies of their passports, their social security numbers, driver’s licenses, birth certificates, and financial information, including his tax returns.” Opp. at 10. But because Mr. Ross does not and cannot allege that AT&T even *had* this information—which was stored in “online accounts”—AT&T plainly could not have disclosed it (much less done so intentionally). See Compl. ¶ 45. As the case law makes clear, later acts of third parties do not satisfy the California Constitution’s invasion of privacy standards. See *Razuki v. Caliber Home Loans, Inc.*, 2018 WL 2761818, at \*1 (S.D. Cal. June 8, 2018) (dismissing an invasion of privacy claim based on hackers’ actions).

**C. The Economic Loss Rule Bars Mr. Ross’s Negligence and Negligent Supervision Claims.**

Mr. Ross also fails to escape the bar to relief presented by the economic loss doctrine. Mr. Ross first argues that AT&T’s contract is one for services, such that the special relationship exception can be applicable.<sup>8</sup> Mr. Ross appears to be appealing to a body of law that finds that where a contract for services is at issue, a plaintiff can fall within the special relationship exception even though the plaintiff and defendant are in privity. See *N. Am. Chem. Co. v. Sup. Ct.*, 59 Cal. App. 4th 764 (1997). But Mr. Ross makes no attempt to rebut AT&T’s reasoning—specifically, that *J’Aire* itself, and the case on which it relies, dealt with a plaintiff who was not in privity with the defendant. Mot. at 14–16; see *Body Jewelz, Inc. v. Valley Forge Ins. Co.*, 241 F. Supp. 3d 1084, 1093 (C.D. Cal. 2017) (“Even the most cursory review of *J’Aire*’s six-factor test reveals that it was not intended for application to parties in privity.”).

Indeed, *J’Aire*’s reasoning makes little sense when divorced from the context in which the court issued it. The very nature of the special relationship exception is to judge whether a party that ordinarily would be unable to sue—because it is a stranger to any contract with the defendant—nonetheless has the type of relationship with the defendant that justifies permitting suit. As AT&T pointed out in its

---

<sup>8</sup> Mr. Ross primarily argues that the “special relationship exception can apply to parties with contracts for services.” Opp. at 10–11. However, he appears to suggest in a footnote that the economic loss rule does not apply at all to contracts for services. That theory would destroy the economic loss rule and has been repeatedly rejected. See *Kalitta Air, L.L.C. v. Cent. Tex. Airborne Sys., Inc.*, 2004 WL 7339814, at \*4 (N.D. Cal. Aug. 19, 2004) (the “economic loss rule applies to the negligent performance of services as well as to the negligent manufacture of goods.”); *Oracle USA, Inc. v. XL Glob. Servs., Inc.*, 2009 WL 2084154, at \*4 (N.D. Cal. July 13, 2009) (the “fundamental rule in California is that no tort cause of action will lie where the breach of duty is nothing more than a violation of a promise which undermines the expectations of the parties to an agreement”).



1 Motion, *all* contracting parties have a relationship. If a contractual relationship were all it took, the  
 2 first factor would *always* favor application of the previously “narrow” and “limited” exception to  
 3 parties in privity. *See Zamora v. Shell Oil Co.*, 55 Cal. App. 4th 204, 211 (1997). This wide application  
 4 would be contrary to the purpose of the economic loss rule, which is to prevent the worlds of contract  
 5 and tort from merging. *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1055 (N.D. Cal. 2014) (Tigar,  
 6 J.) (“Purely economic damages to a plaintiff which stem from disappointed expectations from a  
 7 commercial transaction must be addressed through contract law; negligence is not a viable cause of  
 8 action for such claims.”).

9 Even if a special relationship exception exists where the parties are in privity, Mr. Ross has not  
 10 pled sufficient facts to plausibly allege that he falls within it. For the first factor—whether the contract  
 11 was intended to affect the plaintiff—Mr. Ross argues that AT&T’s Privacy Policy, which was entered  
 12 by “tens of millions of subscribers” (Compl. ¶ 2), was intended to individually affect him. Opp. at 13.  
 13 But if this type of connection were enough to satisfy the factor, it would always be satisfied in cases  
 14 that involve contracting parties. Accordingly, at least in the context of parties in contractual privity,  
 15 this factor requires a plaintiff to be *particularly* affected in a way that is distinguishable from other  
 16 purchasers of goods or services. *See Ott v. Alfa-Laval Agri, Inc.*, 31 Cal. App. 4th 1439, 1455 (1995);  
 17 *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 972 (S.D. Cal.  
 18 2014). Ironically, Mr. Ross even acknowledges that *J’Aire* requires that a transaction “affect the  
 19 plaintiff in a ‘particular’ way,” but only if “the party asserting negligence is a third-party to a contract.”  
 20 Opp. at 12. How could less be required when the parties are in privity? Mr. Ross thus seeks to limit  
 21 the first *J’Aire* factor where parties are not in contractual privity, but then expand it precisely in the  
 22 cases where that expansion would cause the exception to swallow the rule—i.e., cases where the parties  
 23 have a contractual relationship. *J’Aire* does not require such “a radical departure from traditional  
 24 notions of liability.” *Fieldstone Co. v. Briggs Plumbing Prods., Inc.*, 54 Cal. App. 4th 357, 368 (1997).<sup>9</sup>

25 Mr. Ross’s theory that he satisfies the second, third, and fourth factors—the foreseeability of  
 26 \_\_\_\_\_

27 <sup>9</sup> The cases that Mr. Ross cites that appear to lower the standard set by the first factor are conclusory  
 28 in nature and do not analyze the policy and legal reasons that the special relationship exception should  
 not be read to gut the economic loss rule. *See, e.g., Corona v. Sony Pictures Entm’t, Inc.*, 2015 WL  
 3916744, at \*5 (C.D. Cal. June 15, 2015) (analyzing the first factor in two sentences).

1 harm, the degree of certainty that the defendant caused that harm, and the closeness of the connection  
 2 between the defendant's conduct and harm—falters for the same reasons he has not pled proximate  
 3 cause. Because Mr. Ross has not pled the intervening events that connect the alleged SIM swap to his  
 4 alleged harm, it is impossible to evaluate whether those steps are foreseeable. And it is similarly  
 5 impossible to determine whether AT&T's conduct caused any harm, much less the closeness of the  
 6 connection between AT&T's conduct and that alleged harm. Mot. at 4–9, 17; *In re Sony Gaming*  
 7 *Networks*, 996 F. Supp. 2d at 972 (using proximate cause to analyze the third factor).

8 Under the fifth factor—the moral blame assigned to the defendant—Mr. Ross argues that  
 9 AT&T is morally culpable because it knew or should have known that his SIM had been swapped to  
 10 another phone. Opp. at 14. This allegation is insufficient—a plaintiff can only satisfy the fifth *J'Aire*  
 11 factor if the defendant's conduct is “reckless or purposeful.” *Mega RV Corp. v. HWH Corp.*, 225 Cal.  
 12 App. 4th 1318, 1342 (2014). Mr. Ross does not allege that AT&T purposefully or recklessly caused  
 13 his SIM to be swapped—he merely alleges negligence. Compl. ¶¶ 46–70, 95–100; *see also Schneider*,  
 14 151 F.3d at 1197 (holding that only the allegations in the complaint control).

15 For the sixth factor—policy of preventing future harm—Mr. Ross argues that AT&T is culpable  
 16 because it has allegedly done nothing to prevent any future harm. Even if these allegations were in the  
 17 Complaint, which they are not, they are merely attempts to bootstrap other deficient allegations that  
 18 AT&T proximately caused the particular loss claimed in this case. Mr. Ross did not adequately plead  
 19 any initial harm proximately caused by AT&T, so any alleged response to future harm is irrelevant.  
 20 Further, Mr. Ross does not dispute that AT&T already has “strong incentives” to protect its customers’  
 21 data, and his assertion that AT&T has not yet managed to eliminate SIM swaps entirely does not mean  
 22 it lacks such incentives. *Mega RV Corp.*, 225 Cal. App. 4th at 1342.

23 **D. Mr. Ross Cannot Rest on an Inference of Reliance.**

24 Mr. Ross argues that this Court should infer that he relied on AT&T's Privacy Policy, even  
 25 though he never pled that he read it, much less that he read it before he entered his contract with AT&T,  
 26 over a decade before issuance of the Policy he cites. Countless cases have refused to find reliance  
 27 where the plaintiff did not allege that he read, heard, or saw the alleged misrepresentation. Mot. at 19  
 28 n.4; *Opperman*, 87 F. Supp. 3d at 1047 (Tigar, J.) (“What the [complaint] fails to do is connect any



specific Plaintiff to any specific representation. The Court now concludes, even reading the complaint in the light most favorable to Plaintiffs, that Plaintiffs have failed to allege that any one of them saw any particular representation.”). *See also, e.g., Imber–Gluck v. Google, Inc.*, 2014 WL 3600506, at \*5 (N.D. Cal. July 21, 2014); *In re Actimmune Mktg. Litig.*, 2010 WL 3463491, at \*10 (N.D. Cal. Sept. 1, 2010)). Many of those cases rejected an *inference* of reliance for the same reason. In *Rojas-Lozano v. Google, Inc.*, the court rejected an “inference of reliance” because the plaintiff “failed to allege what she saw, what she believed as a result, how knowledge would impact her behavior, or facts that otherwise support a reasonable inference that an omitted fact was material.” 159 F. Supp. 3d 1101, 1114 (N.D. Cal. 2016). And in *Figy v. Amy’s Kitchen, Inc.*, the court held that an inference of reliance requires the plaintiff to allege “at a minimum . . . that he saw the representation at issue.” 2013 WL 6169503, at \*4 (N.D. Cal. Nov. 25, 2013). Here, Mr. Ross did not allege—and does not argue—that he ever read, heard, or even saw AT&T’s Privacy Policy.

Notably, Mr. Ross does not address two of AT&T’s primary arguments. First, AT&T argued that it was impossible for Mr. Ross to rely on the Policy because it was issued *after* Mr. Ross became an AT&T customer. Mot. at 20–21; *see also Daugherty v. Am. Honda Motor Co., Inc.*, 144 Cal. App. 4th 824, 837 n.6 (2006) (“In any event, those representations, such as they were, occurred in 2000 and 2001, not at the time of sale [nearly a decade earlier].”). In essence, Mr. Ross asks this Court to infer that he relied on the 2006 Privacy Policy, even though he alleged nothing about that Policy, including whether it existed, whether it had the same language, or whether he even saw it or read it.

Second, Mr. Ross ignores AT&T’s argument that its Privacy Policy contained important qualifications, which clarified that AT&T could not eliminate the risk that third parties could disclose personal information in violation of the Policy. Mot. at 20. Even if Mr. Ross had pled that he relied on a version of the Policy, he was put on notice that “no security measures are perfect.” Compl., Ex. C at 26. This shortcoming warrants dismissal. *Clayton v. Landsing Pac. Fund, Inc.*, 2002 WL 1058247, at \*6 (N.D. Cal. May 9, 2002) (dismissing a fraudulent concealment claim where the defendant disclosed the allegedly withheld information), *aff’d*, 56 F. App’x 379 (9th Cir. 2003).

#### **E. Mr. Ross’s Alleged Losses Do Not Qualify under the CFAA.**

Mr. Ross’s Opposition does not justify his failure to plead a qualifying loss in the Complaint.

1 First, Mr. Ross alleged—in one sentence—that he “spent in excess of \$5,000 investigating who  
 2 accessed his mobile device and damaged information on it.” Compl. ¶ 202. This allegation is a legal  
 3 conclusion that other courts have repeatedly rejected. Mot. at 22–23; *see DocMagic, Inc. v. Ellie Mae,*  
 4 *Inc.*, 745 F. Supp. 2d 1119, 1150 (N.D. Cal. 2010). Mr. Ross analogizes his allegations to *NovelPoster*  
 5 *v. Javitch Canfield Group*, 140 F. Supp. 3d 954, 963–64 (N.D. Cal. 2014). In *NovelPoster*, the  
 6 plaintiffs, unlike Mr. Ross, alleged “the approximate number of hours that [the plaintiffs] spent on their  
 7 restorative efforts, and the approximate value of their services,” allowing the court to conclude that  
 8 they suffered losses over \$5,000. *Id.* at 963. Far from proving his point, *NovelPoster* undermines it.

9 Second, Mr. Ross argues that his cryptocurrency loss qualifies under the CFAA. Countless  
 10 courts—including this court—reject this argument. The only losses that qualify under the CFAA are  
 11 those that “arise from the investigation or repair of a damaged computer system or data, or from an  
 12 interruption of service.” *Id.* at 963–64. Mere loss of something valuable, like cryptocurrency, is not  
 13 enough—the interruption of service must directly cause the loss. For example, in *SKF USA, Inc. v.*  
 14 *Bjerkness*, the defendants transferred the plaintiff’s data without authorization, causing the plaintiff to  
 15 lose revenue. 636 F. Supp. 2d 696, 721 (N.D. Ill. 2009). While this loss “might fit the usual  
 16 understanding of the term ‘loss,’” the court found that it did not qualify under the CFAA, which  
 17 “provides a different definition that trumps the ordinary definition.” *Id.*; *see also AtPac, Inc. v. Aptitude*  
 18 *Sols., Inc.*, 730 F. Supp. 2d 1174, 1185 (E.D. Cal. 2010) (dismissing CFAA claims where the plaintiff’s  
 19 only loss allegation was that defendants, through their unauthorized access, “obtained something of  
 20 value exceeding \$5,000”).<sup>10</sup>

21 Here, Mr. Ross’s alleged loss of cryptocurrency did not stem from the inability to access his  
 22 SIM card or any other interruption of service. The alleged loss resulted from hackers later obtaining  
 23 something of value after they interrupted his cell phone service. Compl. ¶¶ 24, 37. The interruption  
 24 itself did not cause funds to disappear from his cryptocurrency accounts. Accordingly, Mr. Ross’s  
 25 CFAA claim must be dismissed.

26 \_\_\_\_\_  
 27 <sup>10</sup> Mr. Ross’s best authority for a broader construction of loss is a cursory statement that the CFAA  
 28 provides compensation for lost revenue in a case that contains no discussion of relevant case law. *Tyan,*  
*Inc. v. Garcia*, 2017 WL 1658811, at \*14 (C.D. Cal. May 2, 2017).

**F. Mr. Ross’s Allegations Do Not Support Punitive Damages.**

Finally, Mr. Ross has no colorable defense of his claim for punitive damages. Mr. Ross argues that he has adequately pled that an officer, director, or managing agent of AT&T had advance knowledge of the unfit employee and “employed him or her with a knowing disregard of the rights or safety of others” or authorized or ratified the employee’s conduct. Mot. at 24. Mr. Ross points to his allegation that “AT&T’s Vice President” was aware of SIM swaps and that employees could act in concert with hackers to effect SIM swaps. Opp. at 18. But Mr. Ross’s conclusory allegations do not satisfy the particularity standard required for punitive damage claims. Further, an awareness by AT&T that SIM swaps in general were possible and needed to be confronted is not the same as awareness, much less authorization or ratification, that the alleged SIM swap and resulting theft here would occur.

A “corporation cannot confirm and accept that which it does not actually know about.” *Cruz v. HomeBase*, 83 Cal. App. 4th 160, 168 (2000). To ratify an employee’s conduct, a managing agent must therefore know that the employee was “engaged in harmful activities towards plaintiffs.” *Coll. Hosp. Inc. v. Sup. Ct.*, 8 Cal. 4th 704, 725–26 (1994); *see also Cruz*, 83 Cal. App. 4th at 168 (“There was no evidence that [the defendant’s] officers, directors, or managing agents had actual knowledge that [the two employees] had acted maliciously.”). Here, Mr. Ross not only fails to plead any facts suggesting that any managing agent of AT&T knew of the alleged SIM swap or authorized or ratified it in any way; he actually pleads that the alleged SIM swap was “unauthorized” and against company policy. Compl. ¶¶ 33–34. Accordingly, Mr. Ross has not pled the required authorization or ratification.

Finally, Mr. Ross attempts to circumvent the clear rule that “[m]ere negligence, even gross negligence, . . . [cannot] justify such an award [for punitive damages].” *Toole v. Richardson–Merrell Inc.*, 251 Cal. App. 2d 689 (1967). He argues that *Simplicity Int’l v. Genlabs Corp.*, 2010 WL 11515296, at \*2 (C.D. Cal. Apr. 21, 2010), holds that a claim formally “sounding in negligence” can still lead to punitive damages. The rest of that quote, however, makes clear that the plaintiff must also allege facts showing that the defendant had the “intent to vex, annoy, and injure” or acted in such reckless disregard that its conduct can “be characterized as wanton or willful.” *Id.* Mr. Ross’s allegations do not meet this standard—he offers only the conclusory assertion that AT&T acted with malice, fraud, or oppression “[c]onsidering the allegations of the Complaint as a whole.” Opp. at 19.

But he does not point to a single section of his Complaint showing how AT&T purportedly acted with the required mental state. Instead, he points to distinguishable cases that did contain adequate allegations and asserts that his claims are similarly sufficient, apparently based on nothing more than an alleged awareness by AT&T of SIM swaps. Opp. at 18–19. But Mr. Ross cannot rely on the allegation that AT&T is aware of SIM swaps generally to meet his burden of pleading that AT&T had the mental state required for punitive damages. Awareness of SIM swaps generally is far removed from the intent to “vex, annoy, and injure” Mr. Ross specifically. His conclusory allegations as to mental state are insufficient under *Twombly*. *Perez v. Auto Tech. Co.*, 2014 WL 12588644, at \*7 (C.D. Cal. July 14, 2014).<sup>11</sup>

### III. Conclusion

Mr. Ross has failed to plead facts plausibly suggesting that he is entitled to relief. Accordingly, his Complaint should be dismissed.

Dated: January 22, 2020

MARCELLUS MCRAE  
GIBSON, DUNN & CRUTCHER LLP

By: /s/ Marcellus McRae  
Marcellus McRae

Attorney for Defendant AT&T MOBILITY, LLC

103637494.11

<sup>11</sup> Despite Mr. Ross’s analogy, the allegations in *In re Yahoo!* far exceed those here. *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 313 F. Supp. 3d 1113, 1148 (N.D. Cal. 2018) (detailing acts by high-level officials at Yahoo! who hid or implicitly approved the exact conduct harming the plaintiffs).